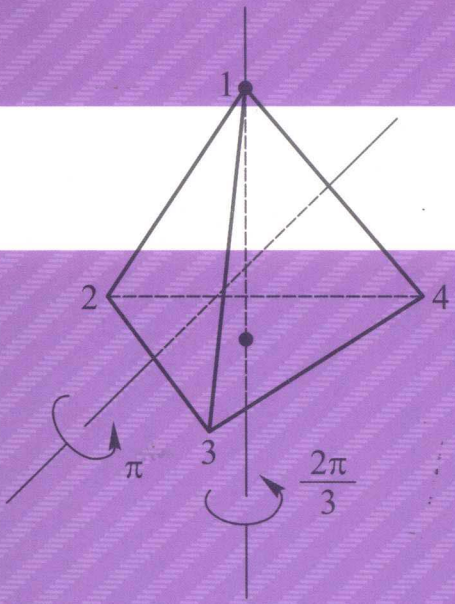

抽象代数基础

（第二版）

丘维声

ABSTRACT ALGEBRA

高等教育出版社

抽象代数基础

Chouxiang Daishu Jichu

（第二版）

丘维声

高等教育出版社·北京

内容提要

本书是大学数学系必修课“抽象代数”(或“近世代数”)课程的教材。全书分三章:第一章群,包括群的典型例子、子群和陪集、群的同构、群的直积、群的同态、正规子群、商群、群在集合上的作用、Sylow 定理、有限 Abel 群的结构、自由群等;第二章环,包括理想、商环、环的同态、环的直和、素理想和极大理想、有限域的构造、Galois 环的构造、分式域、唯一因子分解整环、主理想整环、欧几里得整环等;第三章域扩张及其自同构,包括分裂域、有限域的结构、正规扩张、可分扩张、域扩张的自同构群、Galois 扩张、Galois 基本定理、本原元素、迹与范数等。本书按节配置习题,书末附有习题的提示或答案。

本书根据信息时代的需要精选内容,抓住主线;重视实例和应用,整合知识点;通俗易懂,讲清楚背景和想法;全盘考虑高等代数课和抽象代数课的教学内容,使之成为一个有机整体;注重培养学生科学的思维方式。

本书可作为综合性大学、理工科大学和师范院校数学系的抽象代数(或近世代数)课程的教材,也可作为数学工作者和科技工作者进行科研工作的参考书,还可供学过高等代数课程的读者自学。

图书在版编目(CIP)数据

抽象代数基础/丘维声编著.--2 版.--北京:高等教育出版社,2015.8

ISBN 978-7-04-042642-7

Ⅰ.①抽… Ⅱ.①丘… Ⅲ.①抽象代数-高等学校-教材 Ⅳ.①O153

中国版本图书馆 CIP 数据核字(2015)第 087744 号

策划编辑	田 玲	责任编辑	田 玲	封面设计	李小璐	版式设计	马敬茹
插图绘制	宗小梅	责任校对	刘春萍	责任印制	尤 静		

出版发行	高等教育出版社	网 址	http://www.hep.edu.cn
社 址	北京市西城区德外大街 4 号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.landraco.com
印 刷	北京宏信印刷厂		http://www.landraco.com.cn
开 本	787mm×960mm 1/16		
印 张	12	版 次	2003 年 8 月第 1 版
字 数	210 千字		2015 年 8 月第 2 版
购书热线	010-58581118	印 次	2015 年 8 月第 1 次印刷
咨询电话	400-810-0598	定 价	21.70 元

物 料 号 42642-00

第二版前言

这次修订,改正了个别印刷错误;对第一章§8定理3的证明作了一点修改;对第三章的§2和§3以Galois理论为主线进行了改写;参考文献中增加了一些书目。

作者感谢高等教育出版社编辑李蕊、田玲,她们为本书的编辑出版付出了辛勤的劳动。

作者热忱地欢迎广大读者对本书提出宝贵意见。

丘维声

于北京大学数学科学学院

2014年12月

第一版前言

抽象代数是现代数学的一个重要分支，它主要研究各种代数结构（即，具有代数运算的集合），以及在这些结构中保持运算的映射（称为态射）。抽象代数为现代数学、现代物理学、现代化学、计算机科学、现代通信以及密码学等提供了语言、重要结论和研究方法。当今信息时代，抽象代数有了越来越多的重要应用。抽象代数课程已经成为大学数学系的主干基础课之一。如何教好这门课程？作者根据自己80年代以来在北京大学数学系讲授抽象代数课的体会，把2002年秋季学期给数学科学学院210名学生讲授抽象代数课的讲稿整理成本书，并着重在以下几方面做了一些尝试。

精选内容，抓住主线。我们从信息时代的要求出发，精选抽象代数课程的教学内容。着重讲那些最基本和应用最广泛的内容，讲那些有信息时代气息的内容。全书分成三章：第一章群，第二章环，第三章域扩张及其自同构，对于每一章的内容都抓住主线：第一章的主线是群同态，第二章的主线是理想，第三章的主线是域扩张及其自同构。

重视实例和应用，整合知识点。我们在引言中，从如何度量对称性引出了群的概念，指出群可以用来度量对称性，群可以用来分类几何学，群可以用来判定代数方程能否用根式求解。接着在第一章§1，我们讲了群的典型例子，包括来自数集、几何、代数中群的例子，从中介绍了循环群、二面体群、矩阵群、对称群和交错群等。这使我们在以后各节里可以充分运用这些实例来帮助理解抽象的概念和结论。我们不停留在让学生知道概念的定义上，而且阐述概念的应用。例如在第一章§3，我们从比较二次单位根群 U_2 的乘法表与模2剩余类环 $\mathbf{Z}_2$ 的加法群的加法表，引出了群的同构的概念之后，接着证明了任一无限循环群都与整数加群 $\mathbf{Z}$ 同构，任意一个 m 阶循环群都与 $\mathbf{Z}_m$ 的加法群同构。我们在这一节还决定了4阶群的同构类，并且为了找出一个比较简单的4阶非循环的Abel群，我们引出了群的直积的概念，还证明了 $\mathbf{Z}_m\times\mathbf{Z}_n$ 是循环群当且仅当 $(m,n)=1$，从而可以识别 $\mathbf{Z}_m\times\mathbf{Z}_n$ 是否同构于 $\mathbf{Z}_{mn}$。又如在第二章§3，我们讲了极大理想的概念及其充分必要条件之后，接着讲有限域的构造。进而在§4，我们又讲了代数数域和Galois环的构造。在整本书中，我们从理论的应用的角度，以及内容之间的内在联系的角度，整合了各知识点，把第一章的内容整合成8节，第二章的内容整合成6节，第三章的内容整合成了3节，详见目录。

通俗易懂，讲清楚背景和想法。我们对于重要的概念都要先讲这个概念产生的背景。例如，在第一章§4，我们从茶杯的三视图能反映茶杯的形状这一通俗例子出发，引出了群的同态的概念。在第二章§1，我们从 xOy 平面上的单位圆 C 可看成是圆柱面 $x^2+y^2-1=0$ 与 xOy 平面 $z=0$ 的交，又可看成是单位球面 $x^2+y^2+z^2-1=0$ 与圆柱面 $x^2+y^2-1=0$ 的交等等，引出其零点集包含 C 的所有3元实系数多项式组成的集合 I，并且分析 I 的性质：对减法封闭，有“吸收性”，由此引出理想的概念。我们对于重要的定理，先通过具体例子，猜出可能有的结论，然后进行论证。在论证中特别注意讲清楚关键想法，而且还讲清楚这个关键想法产生的背景，即这个关键想法是怎么想出来的。例如在第一章§7，我们先让学生观察4阶群、9阶群、8阶 Abel 群有多少种互不同构的类型，看出这些 Abel 群都同构于循环群或者若干个循环群的直积，然后问：任意有限 Abel 群是否也有这样的结构？根据 Sylow 第一定理容易把这个问题归结为研究 Abel p-群的结构。在证明 Abel p-群的结构定理之前，我们讲了两个关键想法，并且讲了这两个关键想法是怎么想出来的，然后才讲证明。

全盘考虑高等代数(Ⅰ)(Ⅱ)和抽象代数课程的教学内容，使之成为一个有机整体。高等代数(Ⅰ)(Ⅱ)和抽象代数是大学数学系在代数方面的必修课，共三个学期。作者在去年下半年给数学科学学院本科生讲授抽象代数课时，对于抽象代数课与高等代数(Ⅰ)(Ⅱ)的教学内容作了统筹安排，对作者编写的《高等代数(上册、下册)》进行了修订，同时详细写了抽象代数每一次大课的讲稿。大体上说，高等代数(Ⅰ)讲授线性代数的具体部分，内容包括：线性方程组、行列式、数域 K 上 n 元有序数组的向量空间 K^n、矩阵的运算、K^n 到 K^s 的线性映射(即，$A\alpha=A\alpha$)、欧几里得空间 $\mathbf{R}^n$、矩阵的相抵分类、矩阵的相似以及矩阵的特征值和特征向量、二次型与矩阵的合同。高等代数(Ⅱ)讲授多项式环(着重讲一元多项式环的理论)，介绍模 m 剩余类环 $\mathbf{Z}_m$ 和模 p 剩余类域 $\mathbf{Z}_p$，以及域的特征；讲授线性代数的抽象部分，内容包括：域上的线性空间、线性映射(包括线性变换和线性函数)、具有度量的线性空间(包括欧几里得空间、酉空间，以及正交空间和辛空间简介)。抽象代数讲授群的结构、环的结构、域扩张及其自同构。我们努力使这三个学期的代数课程成为一个有机整体。例如，我们在《高等代数(第二版)下册》的第七章§8详细讨论了 $\mathbf{Q}[x]$ 中本原多项式的性质，证明了每一个次数大于0的本原多项式可以唯一地分解成 $\mathbf{Q}$ 上不可约的本原多项式的乘积。这样我们在本书的第二章§6中，利用上述结论很容易地得出，$\mathbf{Z}[x]$ 中每一个次数大于0的本原多项式可以唯一地分解成 $\mathbf{Z}$ 上不可约的本原多项式的乘积，进而证明了 $\mathbf{Z}[x]$ 是唯一因子分解整环，即 Gauss 整环。接着我们指出，上述证明 $\mathbf{Z}[x]$ 是 Gauss 整环的方法也可用于证明下述结论：Gauss 整环 R 上

的一元多项式环 $R[x]$ 也是 Gauss 整环。这样不仅节省了教学时间，而且使高等代数课与抽象代数课的教学内容前后呼应，有利于学生对抽象理论的理解。

注重培养学生科学的思维方式。我们认为讲授一门课程不仅要让学生掌握本门课程的基本知识、基本方法，受到本门课程的基本训练，而且要培养学生具有科学的思维方式。数学的思维方式就是一种科学的思维方式。我们把数学的思维方式概括为：观察客观现象，抓住其主要特征，抽象出概念或者建立模型；进行探索，通过直觉判断或者归纳推理、类比推理以及联想等作出猜测；然后进行深入分析和逻辑推理以及计算，揭示事物的内在规律，从而使纷繁复杂的现象变得井然有序。这就是数学思维方式的全过程。我们按照数学思维方式讲课，可以使学生从中受到熏陶，既使他们比较顺利地学好目前的课程，又有助于他们把今后肩负的工作做好。

本书的每一节都配备了习题，书末附有习题的提示或答案。

本书可作为综合性大学、理工科大学和师范院校的数学系抽象代数（或近世代数）课程的教材。书中加“*”号的内容和用楷体字排印的内容不作为教学要求，供有兴趣的读者自己看。

作者感谢本书的责任编辑胡乃冏编审，他为本书的编辑出版付出了辛勤的劳动。

作者热忱地欢迎广大读者对本书提出宝贵意见。

丘维声

于北京大学数学科学学院

2003 年 5 月

目　录

引　言

一、抽象代数的研究对象

自然界和现实生活中，美丽的蝴蝶、多姿的雪花、绚丽的墙纸、耀眼的窗花……无不具有对称性，而使人心旷神怡.

如何度量对称性(symmetry)？

例如，我们很容易看出，等边三角形比等腰三角形(它的腰与底不相等)更具有对称性，道理是什么呢？

设等腰三角形底边上的垂直平分线为 l(图 0-1)，则平面上关于 l 的反射 τ 把等腰三角形变成与它自己重合的图形.显然，平面的恒等变换 I 也具有这个性质.

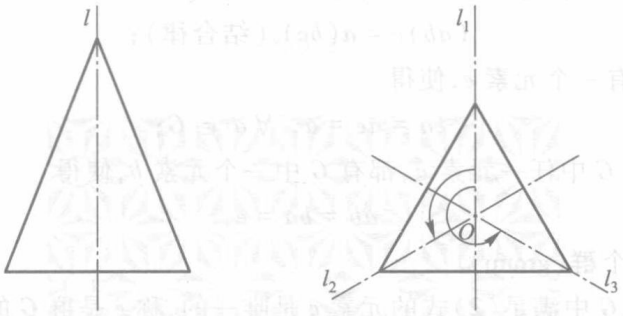

图 0-1

设等边三角形(equilateral triangle)的中心为 O，三条边上的垂直平分线分别为 l_1, l_2, l_3(图 0-1).则平面上关于 l_i 的反射 τ_i 把等边三角形变成与它自己重合的图形，$i=1,2,3$；平面上绕点 O 的转角分别为 $\frac{2\pi}{3}, \frac{4\pi}{3}$ 的旋转 σ_1, σ_2，以及恒等变换 I 也具有这个性质.

平面上(或空间中)的正交(点)变换(也称保距变换(isometry))，如果把平面(或空间)图形 Γ 变成与它自己重合的图形，则把这个正交(点)变换叫做图形 Γ 的**对称(性)变换**.

上面指出，等边三角形的对称(性)变换已经有 6 个.进一步可以证明，只有这 6 个.类似地，等腰三角形(它的腰与底不相等)的对称(性)变换有且只有两个.我们自然可以说：等边三角形比等腰三角形更具有对称性.

我们把等边三角形的所有对称(性)变换组成一个集合:

$$G=\{I,\sigma_1,\sigma_2,\tau_1,\tau_2,\tau_3\}.$$

我们知道,平面上两个正交(点)变换的乘积仍是正交(点)变换;并且如果它们都把等边三角形变成与它自己重合的图形,那么它们的乘积也有这个性质.因此等边三角形的任意两个对称(性)变换的乘积仍是它的对称(性)变换.从而集合 G 对于映射的乘法封闭.因此映射的乘法是集合 G 上的一个(二元)代数运算.

一般地,非空集合 S 与自己的笛卡儿积 $S\times S$ 到 S 的一个映射,称为 S 上的一个**二元代数运算**,简称为 S 上的代数运算.

由于映射的乘法适合结合律,因此上述集合 G 上的代数运算适合结合律.

G 中有恒等变换 I,I 与 G 中任一元素的乘积(左乘或右乘)都等于该元素自己.

容易看出,G 中每个变换都有逆变换.例如,$\sigma_1^{-1}=\sigma_2$,$\tau_i^{-1}=\tau_i$,$i=1,2,3$.

从上面的例子以及大量类似的例子,我们抽象出下述概念:

定义 1 设 G 是一个非空集合,如果在 G 上定义了一个代数运算,通常称为乘法,记作 ab,并且它适合下列条件:

(i) 对于 G 中任意元素 a,b,c,有

$$(ab)c=a(bc)\ (\text{结合律});\tag{1}$$

(ii) G 中有一个元素 e,使得

$$ea=ae=a,\ \forall a\in G;\tag{2}$$

(iii) 对于 G 中任一元素 a,都有 G 中一个元素 b,使得

$$ab=ba=e,\tag{3}$$

那么 G 称为一个**群**(group).

容易说明,G 中满足(2)式的元素 e 是唯一的,称 e 是群 G 的**单位元**(identity element);对于 G 中元素 a,G 中满足(3)式的元素 b 是唯一的,称 b 是 a 的**逆元**(inverse),记作 a^{-1}.于是(3)式可以写成

$$aa^{-1}=a^{-1}a=e.\tag{4}$$

从(4)式看出,a^{-1}的逆元是 a,即$(a^{-1})^{-1}=a$.

群 G 的运算也可以称为加法,记作 $a+b$,此时结合律为

$$(a+b)+c=a+(b+c),\quad \forall a,b,c\in G;$$

单位元称为零元,记成 0;a 的逆元称为 a 的负元,记成$-a$.

如果群 G 的运算还适合交换律,即对于 G 中任意元素 a,b,有 $ab=ba$,则称 G 为**交换群**(或 **Abel(阿贝尔)群**).

从上面的讨论知道,等边三角形的所有对称(性)变换组成的集合 G,对于映射的乘法成为一个群.用类似的方法可以说明:

图形 Γ 的所有对称(性)变换组成的集合 G,对于映射的乘法成为一个群,

称 G 是**图形 Γ 的对称(性)群**(symmetry group).

上述表明,群可以用来度量对称性.

用群来度量对称性的重要意义在于:我们可以通过研究群的分类,来对具有对称性的客观事物进行分类.

例如,现实生活中,常常用正方形或正六边形的砖铺地面,如图 0-2;也常常用具有对称性图案的纸贴墙壁,如图 0-3.

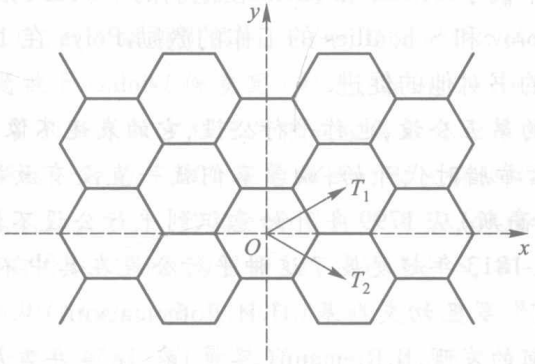

图 0-2

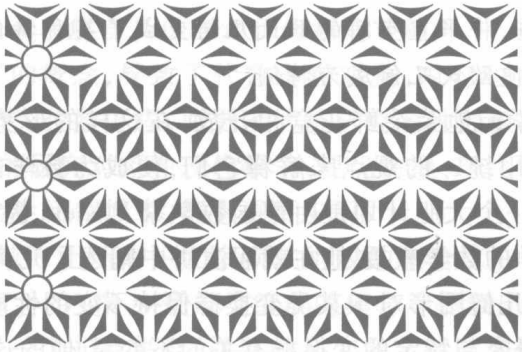

图 0-3

设想这些图案分别铺满了整个平面.如果铺满了图案的平面的对称(性)群不固定一个点,也不固定一条直线,则称它为**平面晶体群**(plane crystallographic group)(或者称为**贴墙纸群**(wallpaper group)). R.Fricke 和 F.Klein(克莱因)在他们关于自同构函数的第一本书(1897)中,对平面晶体群进行分类.G.Pólya(波利亚)在 1924 年发表的一篇文章中,完成了对平面晶体群的分类:共有 17 种不同的平面晶体群,并且给出了相应的装饰图案式样的例子.

自然界中有各种各样的晶体,每一种晶体的原子结构的模型可以看成是空间中的点阵.设想将这种点阵连续地、无限地填充整个空间.填充了点阵的空间

的对称(性)群,如果既不固定一个点,也不固定一条直线,而且不固定一个平面,则称它为**空间晶体群**(space crystallographic group).对空间晶体群进行分类,就可以了解自然界中各种晶体的结构.在1868年,C.Jordan(若尔当)借助Bravais(1848)对晶体结构分类的工作,研究空间晶体群的分类,虽然没有完全分类,但是这为E.S.Fedorov(1890)和A.Schönflies(1891)的工作铺平了道路.Fedorov和Schönflies分别独立地证明了空间晶体群共有230个.这是历史上将群论直接用于自然科学的第一个例子.Fricke和Klein在他们的书(1897)中对平面晶体群的分类,就是受到Fedorov和Schönflies的工作的激励.Pólya在1924年发表的文章中,感谢Schönflies的书对他的促进.

欧几里得几何的第五公设,也称平行公设,它的表述不像其他4条公设那样简洁、明了.因此从古希腊时代开始,数学家们就一直没有放弃消除对第五公设质疑的努力,Gauss(高斯)从1799年开始意识到平行公设不能从其他的欧几里得公理推出来,并从1813年起发展了这种平行公设在其中不成立的新几何,称为"非欧几里得几何".罗巴切夫斯基(Н.И.Лобачевский)从1826年开始,报告了自己关于非欧几何的发现.B.Riemann(黎曼)在1854年发展了罗巴切夫斯基等人的思想而建立了一种更广泛的几何,即现在所称的黎曼几何,罗巴切夫斯基的非欧几何和通常的欧几里得几何是黎曼几何中的两种特殊情形.非欧几何揭示了空间的弯曲性质,将平直空间的欧氏几何变成了某种特例.而射影几何的发展,又从另一个方向使欧氏几何成为特例.

19世纪的几何学园地朵朵鲜花竞相开放,在这样的形势下,寻找不同几何学之间的内在联系,用统一的观点来解释它们,便成为数学家们追求的一个目标.统一几何学的第一个大胆计划是由德国数学家F.Klein提出的.1872年,Klein被聘为爱尔朗根大学的数学教授.他在就职演讲中阐述了几何学统一的思想:所谓几何学,就是研究几何图形对于某类变换群保持不变的性质的学问,或者说任何一种几何学只是研究与特定的变换群有关的不变量.他的这次演讲被称为《爱尔朗根纲领(Erlangen Program)》.欧几里得几何就是研究图形在正交(点)变换群下保持不变的性质,而研究图形在仿射变换群下保持不变的性质的几何,称为仿射几何;研究图形在射影变换群下保持不变的性质的几何,称为射影几何.(关于正交(点)变换、仿射变换、射影变换的概念可以参看参考文献[12].)

上述表明,群可以用来分类几何学.

二次方程的解法古巴比伦人就已掌握,16世纪左右由S.Ferro,N.F.Tartaglia,G.Cardano,L.Ferrari先后给出了三次、四次方程的根式解.此后人们便着力研究高次方程(即,五次和五次以上的方程)的根式解问题.到了18世纪,J.L.Lagrange(拉格朗日)在1770年发表长篇论文《关于代数方程解的思考》.他在

其中探讨一般三次、四次方程能用根式求解的原因.在1799年,P.Ruffini(鲁菲尼)明确提出要证明高于四次的一般方程不可能用代数方法求解.到了19世纪,N.H.Abel在1824年自费出版了一本小册子《论代数方程,证明一般五次方程的不可解性》,在其中严格证明了以下事实:如果方程的次数 $n\geqslant 5$,并且系数 a_1,a_2,$\cdots$,a_n 看成是字母,那么任何一个由这些字母组成的根式都不可能是方程

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \tag{5}$$

的根.这样,五次和高于五次的一般方程不能用根式求解的问题就由Abel解决了.在Abel的工作之后,数学家所面临的一个问题是:什么样的特殊方程能够用根式求解?这个问题被E.Galois(伽罗瓦)解决,Galois在1829—1831年间完成的几篇论文中,建立了判别代数方程可用根式求解的充分必要条件,从而宣告了代数方程用根式求解这一经历了300年的难题的彻底解决.Galois的思想是将 n 次方程(5)的 n 个根 $x_1,x_2,\cdots,x_n$ 作为一个整体来考察,令 $\Omega=\{x_1,x_2,\cdots,x_n\}$,$\Omega$ 上的所有置换(Ω 到自身的双射称为置换)组成的集合 S_n 有一个代数运算:置换的乘法(即,映射的乘法).Galois称 S_n 为"群".这是历史上最早的"群"的定义,不过它只是针对一个具体的群(置换群)所作的定义,还不是抽象群的一般定义.Galois进一步考虑 S_n 中某些置换组成的"子群",他称之为"方程的群",也就是我们今天所说的"Galois群".方程的群刻画了方程的根的对称性.Galois证明了:方程 $f(x)=0$ 可用根式求解当且仅当方程的群是可解群.

Galois引进"群"的概念,导致了代数学在对象、内容和方法上的深刻变革.代数学不再仅仅是研究代数方程,而更多的是研究各种抽象的"对象"的运算关系,代数学的这些新的研究对象在现代数学、现代物理、现代化学以及通信科学、信息安全等现代社会生活领域中,都有重要应用.

从整数集 $\mathbf{Z}$,数域 K 上所有一元多项式组成的集合 $K[x]$,数域 K 上所有 n 级矩阵组成的集合 $M_n(K)$,模 m 剩余类组成的集合等抽象出环的概念.

定义2　设 R 是一个非空集合,如果在 R 上定义了两个代数运算,一个叫加法,记为 $a+b$;另一个叫乘法,记为 ab,并且它们适合下列条件:

(i) R 对于加法成一个交换群;

(ii) 乘法的结合律:对 R 中任意元素 a,b,c,有

$$(ab)c = a(bc);$$

(iii) 乘法对加法的分配律:对所有的 $a,b,c\in R$,有

$$a(b+c) = ab + ac \quad \text{(左分配律)},$$

$$(b+c)a = ba + ca \quad \text{(右分配律)},$$

那么 R 称为一个**环**(ring).

如果环 R 的乘法还适合交换律,则称 R 为**交换环**(commutative ring).

如果环 R 中有一个元素 e 具有性质：对于 R 中任意元素 a，有 $ae=ea=a$，则称 e 是 R 的**单位元**，称 R 是有单位元的环，通常把 R 的单位元就记成 1.

在有单位元的环 R 中，对于元素 a，如果 R 中有元素 b，使得 $ab=ba=1$，则称 a 是**可逆元**(invertible element)(或**单位**(unit))，此时把 b 称为 a 的**逆元**，记成 a^{-1}.(注：可以说明，如果 a 是可逆元，则满足 $ab=ba=1$ 的元素 b 是唯一的.)

定义 3 如果 F 是一个有单位元 $1(\neq 0)$ 的交换环，并且它的每一个非零元都可逆，则称 F 是一个**域**(field).

从域的定义看出，域 F 有两个代数运算：加法和乘法，并且 F 对于加法成一个交换群，F 的所有非零元组成的集合 F^* 对于乘法也成一个交换群，并且适合乘法对于加法的分配律.

有理数域 $\mathbf{Q}$，实数域 $\mathbf{R}$，复数域 $\mathbf{C}$ 等数域都是域.

可以证明：当 p 为素数时，模 p 剩余类环 $\mathbf{Z}_p$ 是一个域(证明参看参考文献[14]，第 69 页).称 $\mathbf{Z}_p$ 是模 p 剩余类域.一个域如果只有有限个元素，则称它为**有限域**.

有限域在现代通信和信息安全中有重要应用.

像群、环、域那样，具有代数运算的集合称为**代数结构**(algebraic structure).

抽象代数(abstract algebra)的研究对象是代数结构，并且是通过研究保持运算的映射(称为**态射**(morphism))来研究代数结构.

抽象代数使代数结构和态射成为代数学研究的中心.

二、抽象代数的重要性

抽象代数为现代数学、现代物理学、现代化学以及计算机科学、现代通信和密码学等提供了语言.

抽象代数研究结构和态射的思想已经渗透到现代数学的各个分支中.在很多数学对象的研究中都要首先建立适当的代数结构或其他结构，然后通过研究态射来研究这些结构.

抽象代数的研究方法和重要结论在现代数学的各个分支，以及现代物理学、计算机科学、通信科学、信息安全、经济学等领域都有重要应用.

学习抽象代数可以受到数学思维方式的很好的训练，从而在培养科学的思维方式上有质的提高.

三、抽象代数的学习方法

1. 要按照数学的思维方式来学习抽象代数.

什么是数学的思维方式？观察客观世界的现象，抓住其主要特征，抽象出概念或者建立模型；进行探索，通过直觉判断或者归纳推理、类比推理以及联想等

作出猜测;然后进行深入分析和逻辑推理以及计算,揭示事物的内在规律,从而使纷繁复杂的现象变得井然有序.这就是数学的思维方式.

2. 要多用具体例子来理解抽象代数的概念和结论.

3. 要抓住抽象代数研究代数结构,并且通过研究态射来研究代数结构这条主线.

4. 要在理解的基础上记住基本概念和重要结论.

5. 要运用抽象代数的研究方法和重要结论去解决具体问题.

6. 要做一定数量的习题,才能理解概念、掌握理论和提高分析问题的能力.

习　题

1. 证明:在群 G 中,对于任意元素 a,b,方程 $ax=b$ 有唯一解;方程 $ya=b$ 也有唯一解.

2. 证明:在群 G 中,消去律成立.即

由 $ax = ay$ 可以推出 $x = y$;

由 $xa = ya$ 可以推出 $x = y$.

3. 模 4 剩余类环 $\mathbf{Z}_4$ 中,所有非零元组成的集合对于乘法是否成为一个群?

4. 求出 $\mathbf{Z}_8$ 中的所有可逆元.

5. 证明:在模 m 剩余类环 $\mathbf{Z}_m$ 中,$\bar{a}$ 可逆当且仅当$(a,m)=1$.

第一章　群

§1　群的典型例子：循环群，二面体群，矩阵群，对称群

一个群是指一个非空集合 G，它满足下列 4 个条件：

(i) 在 G 上定义了一个(二元)代数运算；

(ii) G 上的运算适合结合律；

(iii) G 中有一个元素 e，具有下述性质：

$$ae = ea = a, \quad \forall a \in G,$$

称 e 是 G 的单位元；

(iv) G 中每一个元素都有逆元.

如果 G 满足条件(i)(ii)，则称 G 为**半群**(semigroup)；如果 G 满足条件(i)(ii)(iii)，则称 G 为**幺半群**(monoid).

群 G 中不同元素的逆元是不同的.这是因为如果 G 中，$a^{-1}=b^{-1}$，则 $(a^{-1})^{-1}=(b^{-1})^{-1}$，从而 $a=b$.

容易验证，群 G 中，有

$$(ab)^{-1} = b^{-1}a^{-1}. \tag{1}$$

由于群 G 的运算适合结合律，因此 n 个元素 $a_1, a_2, \cdots, a_n$ 的乘积是唯一确定的，把它记作 $a_1a_2\cdots a_n$.容易验证：

$$(a_1a_2\cdots a_n)^{-1} = a_n^{-1}\cdots a_2^{-1}a_1^{-1}. \tag{2}$$

群 G 中，n 个 a 的乘积记作 a^n，读作“a 的 n 次幂”.即

$$a^n \xlongequal{\text{def}} \underbrace{aa\cdots a}_{n\text{个}}, \quad n \in \mathbf{Z}^+. \tag{3}$$

我们还规定：

$$a^0 \xlongequal{\text{def}} e, \tag{4}$$

$$a^{-n} \xlongequal{\text{def}} (a^{-1})^n, \quad n \in \mathbf{Z}^+. \tag{5}$$

容易验证：

$$a^n a^m = a^{n+m}, \quad n, m \in \mathbf{Z}; \tag{6}$$

$$(a^n)^m = a^{nm}, \quad n, m \in \mathbf{Z}. \tag{7}$$